ROZDÍLOVÁ TABULKA NÁVRHU PRÁVNÍHO PŘEDPISU S PŘEDPISY EU

Navrhovaný právní předpis		Odpovídající předpis EU		
Ustanovení (část, §, odst., písm., apod.)	Obsah	Celex č.	Ustanovení (čl., odst., písm., bod, apod.)	Obsah
§ 1 odst. 2	(2) Tento zákon zapracovává příslušné předpisy Evropské unie[6)] (dále jen „Unie“) a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. _____ 6) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.	32016L1148	Čl. 25 odst. 1	1. Členské státy do ... [21 měsíců ode dne vstupu této směrnice v platnost] přijmou a zveřejní právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí. Znění těchto předpisů neprodleně sdělí Komisi. Použijí tyto předpisy ode dne … [den následující po dni uvedeném v prvním pododstavci]. Tyto předpisy přijaté členskými státy musí obsahovat odkaz na tuto směrnici nebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsob odkazu si stanoví členské státy.
§ 2 písm. c)	c) bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací a dat,	32016L1148	Čl. 4 odst. 2	2) „bezpečností sítí a informačních systémů“ schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné;
§ 2 písm. i) až m)	i) základní službou služba, jejíž poskytování je	32016L1148	Čl. 4 odst. 4	4) „provozovatelem základních služeb“ veřejný

	závislé na sítích elektronických komunikací[7)] nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví 1. energetika, 2. doprava, 3. bankovnictví, 4. infrastruktura finančních trhů, 5. zdravotnictví, 6. vodní hospodářství, 7. digitální infrastruktura, 8. chemický průmysl, j) informačním systémem základní služby informační systém, na jehož fungování je závislé poskytování základní služby, k) provozovatelem základní služby orgán nebo osoba, která poskytuje základní službu a která je určena Národním bezpečnostním úřadem (dále jen „Úřad“) podle § 22a; pro účely plnění informační povinnosti podle příslušného předpisu Evropské unie8) se za provozovatele základní služby považují též orgány a osoby uvedené v § 3 písm. c) a d),		až 6	nebo soukromý subjekt, jehož druh je uveden v příloze II a jenž splňuje kritéria stanovené v čl. 5 odst. 2; 5) „digitální službou“ služba ve smyslu čl. 1 odst. 1 písm. b) směrnice Evropského parlamentu a Rady (EU) 2015/1535[1], jejíž druh je uveden v příloze III; 6) „poskytovatelem digitálních služeb“ jakákoli právnická osoba poskytující digitální službu;

[1] Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (Úř. věst. L 241, 17.9.2015, s. 1).

	l) digitální službou služba informační společnosti podle zákona upravujícího některé služby informační společnosti[9)], která spočívá v provozování 1. on-line tržiště, které spotřebiteli nebo prodávajícímu umožňuje on-line uzavírat s prodávajícím podnikatelem[10)] kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, který využívá službu poskytovanou on-line tržištěm, 2. internetového vyhledávače, který umožňuje provádět vyhledávání v zásadě na všech internetových stránkách, a to na základě dotazu uživatele na jakékoliv téma v podobě klíčového slova, sousloví nebo jiného zadání, přičemž služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem, nebo 3. cloud computingu, který umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet, a m) příslušným orgánem orgán vykonávající působnost v oblasti kybernetické bezpečnosti.			

	_____ 7) § 2 písm. h) zákona č. 127/2005 Sb., ve znění pozdějších předpisů. 8) Čl. 5 odst. 7 směrnice Evropského parlamentu a Rady (EU) 2016/1148. 9) § 2 písm. a) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). 10) § 2 odst. 1 písm. a) a b) zákona č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů. § 419 a 420 zákona č. 89/2012 Sb., občanský zákoník.			
			Čl. 4 odst. 17	17) „on-line tržištěm“ digitální služba, která spotřebitelům ve smyslu čl. 4 odst. 1 písm. a) směrnice Evropského parlamentu a Rady 2013/11/EU[2] a obchodníkům ve smyslu čl. 4 odst. 1 písm. b) uvedené směrnice, umožňuje uzavírat s obchodníky on-line smlouvy o prodeji a o poskytnutí služeb, a to prostřednictvím internetových stránek on-line tržiště nebo prostřednictvím internetových stránek obchodníka, jež využívají výpočetních služeb poskytovaných on-line tržištěm;

[2] Směrnice Evropského parlamentu a Rady 2013/11/EU ze dne 21. května 2013 o alternativním řešení spotřebitelských sporů a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (směrnice o alternativním řešení spotřebitelských sporů) (Úř. věst. L 165, 18.6.2013, s.63).

			Čl. 4 odst. 19	„službou cloud computingu“ digitální služba umožňující přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, které je možno sdílet;
			Čl. 16 odst. 11	11. Kapitola V se nevztahuje na mikropodniky a malé podniky ve smyslu doporučení Komise 2003/361/ES[3].
			Čl. 5 odst. 1	Do 9. listopadu 2018 členské státy v každém odvětví a pododvětví uvedeném v příloze II určí provozovatele základních služeb usazené na jejich území.
			Čl. 5 odst. 2	2. Kritéria pro určení provozovatele základních služeb podle čl. 4 bodu 4 jsou tato: a) subjekt poskytuje službu, která je základní z hlediska zachování kritických společenských nebo ekonomických činností; b) poskytování dotyčné služby je závislé na sítích a informačních systémech a c) incident by vedl k významnému narušení poskytování této služby.
			Čl. 1 odst. 2 písm. e)	Za tímto účelem tato směrnice: e) ukládá členským států povinnost určit vnitrostátní příslušné orgány, jednotná kontaktní místa a týmy CSIRT, jejichž úkoly budou souviset s bezpečností sítí a informačních systémů.
			Čl. 8 odst. 1	1. Každý členský stát určí jeden nebo více vnitrostátních příslušných orgánů v oblasti

[3] Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

				bezpečnosti sítí a informačních systémů (dále jen „příslušný orgán“) alespoň pro odvětví podle přílohy II a služby podle přílohy III. Členské státy mohou tuto úlohu svěřit již existujícímu orgánu nebo orgánům.
			Článek 14 odst. 7	7. Příslušné orgány jednající společně v rámci skupiny pro spolupráci mohou vypracovat a přijmout pokyny týkající se okolností, za nichž jsou provozovatelé základních služeb povinni hlásit incidenty, včetně parametrů pro určení významnosti dopadu daného incidentu, jak je uvedeno v odstavci 4.
			Příloha III	Druhy digitálních služeb pro účely čl. 4 bodu 5. 1. On-line tržiště 2. Internetový vyhledávač 3. Služba cloud computingu
			Příloha II	Druhy subjektů pro účely čl. 4 bodu 4 *1. Energetika* *a) elektřina* – elektroenergetické podniky ve smyslu čl. 2 bodu 35 směrnice Evropského parlamentu a Rady 2009/72/ES[4], které zastávají funkci „dodávky“ ve smyslu čl. 2 bodu 19 uvedené směrnice – provozovatelé distribuční soustavy ve

[4] Směrnice Evropského parlamentu a Rady 2009/72/ES ze dne 13. července 2009 o společných pravidlech pro vnitřní trh s elektřinou a o zrušení směrnice 2003/54/ES (Úř. věst. L 211, 14.8.2009, s. 55).

				smyslu čl. 2 bodu 6 směrnice 2009/72/ES – provozovatelé přenosové soustavy ve smyslu čl. 2 bodu 4 směrnice 2009/72/ES *b) ropa* – provozovatelé ropovodů – provozovatelé zařízení na těžbu, rafinaci a zpracování ropy a skladovacích a přenosových zařízení *c) zemní plyn* - dodavatelské podniky ve smyslu čl. 2 bodu 8 směrnice Evropského parlamentu a Rady 2009/73/ES;[5] – provozovatelé distribuční soustavy ve smyslu čl. 2 bodu 6 směrnice 2009/73/ES – provozovatelé přepravní soustavy ve smyslu čl. 2 bodu 4 směrnice 2009/73/ES – provozovatelé skladovacího zařízení ve smyslu čl. 2 bodu 10 směrnice 2009/73/ES – provozovatelé zařízení LNG ve smyslu čl. 2 bodu 12 směrnice 2009/73/ES – plynárenské podniky ve smyslu čl. 2 bodu 1 směrnice 2009/73/ES – provozovatelé zařízení na rafinaci a zpracování zemního plynu

[5] Směrnice Evropského parlamentu a Rady 2009/73/ES ze dne 13. července 2009 o společných pravidlech pro vnitřní trh se zemním plynem a o zrušení směrnice 2003/55/ES (Úř. věst. L 211, 14.8.2009, s. 94).

				2. Doprava *a) letecká doprava* - letečtí dopravci ve smyslu čl. 3 bodu 4 nařízení Evropského parlamentu a Rady (EU) č. 300/2008[6] – řídící orgány letiště ve smyslu čl. 2 bodu 2 směrnice Evropského parlamentu a Rady 2009/12/ES[7], letiště ve smyslu čl. 2 bodu 1 uvedené směrnice, včetně hlavních letišť uvedených v příloze II, části 2 nařízení Evropského parlamentu a Rady č. 1315/2013[8]; a subjekty provozující pomocná zařízení v rámci letišť - provozovatelé kontroly řízení provozu poskytující službu řízení letového provozu ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 549/2004[9] *b) železniční doprava* – provozovatelé infrastruktury ve smyslu čl. 3 bodu 2 směrnice Evropského parlamentu a Rady 2012/34/EU - železniční podniky ve smyslu čl. 3 bodu 1 směrnice 2012/34/EU, včetně provozovatelů

6 Nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy a o zrušení nařízení (ES) č. 2320/2002 (Úř. věst. L 97, 9.4.2008, s. 72).

7 Směrnice Evropského parlamentu a Rady 2009/12/ES ze dne 11. března 2009 o letištních poplatcích (Úř. věst. L 70, 14.3.2009, s. 11).

8 Nařízení Evropského parlamentu a Rady (EU) č. 1315/2013 ze dne 11. prosince 2013 o hlavních směrech Unie pro rozvoj transevropské dopravní sítě a o zrušení rozhodnutí č. 661/2010/EU (Úř. věst. L 348, 20.12.2013, s. 1).

9 Nařízení Evropského parlamentu a Rady (ES) č. 549/2004 ze dne 10. března 2004, kterým se stanoví rámec pro vytvoření jednotného evropského nebe (rámcové nařízení) (Úř. věst. L 96, 31.3.2004, s. 1).

				zařízení služeb ve smyslu čl. 3 bodu 12 směrnice 2012/34/EU *c)* vodní *doprava* – společnosti vnitrozemské, námořní a pobřežní osobní a nákladní vodní dopravy, jak jsou vymezeny pro námořní dopravu v příloze I nařízení Evropského parlamentu a Rady (ES) č. 725/2004[10], kromě jednotlivých plavidel provozovaných těmito podniky - řídící orgány přístavů ve smyslu čl. 3 bodu 1 směrnice Evropského parlamentu a Rady 2005/65/ES[11], včetně jejich přístavních zařízení ve smyslu čl. 2 bodu 11 nařízení (ES) č. 725/2004; a subjekty provozující díla a zařízení v rámci přístavů – provozovatelé služeb lodní dopravě ve smyslu čl. 3 písm. o) směrnice Evropského parlamentu a Rady 2002/59/ES *d) silniční doprava* - silniční orgány ve smyslu čl. 2 bodu 12 nařízení Komise v přenesené pravomoci (EU) 2015/962[12] odpovědné za kontrolu řízení provozu. – provozovatelé inteligentních dopravních systémů ve smyslu čl. 4 bodu 1 směrnice

[10] Nařízení Evropského parlamentu a Rady (ES) č. 725/2004 ze dne 31. března 2004 o zvýšení bezpečnosti lodí a přístavních zařízení (Úř. věst. L 129, 29.4.2004, s. 6).

[11] Směrnice Evropského parlamentu a Rady 2005/65/ES ze dne 26. října 2005 o zvýšení zabezpečení přístavů, Úř. věst. L 310, 25.11.2005, s. 28.

[12] Nařízení Komise v přenesené pravomoci (EU) 2015/962 ze dne 18. prosince 2014 , kterým se doplňuje směrnice Evropského parlamentu a Rady 2010/40/EU, pokud jde o poskytování informačních služeb o dopravním provozu v reálném čase v celé EU (Úř. věst. L 157, 26.3.2015, s. 21).

				Evropského parlamentu a Rady 2010/40/EU[13] *3. Bankovnictví* - úvěrové instituce ve smyslu čl. 4 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 575/2013[14] *4. Infrastruktura finančních trhů* – provozovatelé obchodních systémů ve smyslu čl. 4 bodu 24 směrnice Evropského parlamentu a Rady 2014/65/EU[15] – ústřední protistrany ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 648/2012[16] *5. Zdravotnictví* zdravotnická zařízení (včetně nemocnic a soukromých klinik) - poskytovatelé zdravotní péče ve smyslu čl. 3 písm. g) směrnice Evropského parlamentu a Rady

[13] Směrnice Evropského parlamentu a Rady 2010/40/EU ze dne 7. července 2010 o rámci pro zavedení inteligentních dopravních systémů v oblasti silniční dopravy a pro rozhraní s jinými druhy dopravy (Úř. věst. L 207, 6.8.2010, s. 1).

[14] Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012 – Úř. věst. L 176, 27.6.2013, s. 1.

[15] Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU (Úř. věst. L 173, 12.6.2014, s. 349)

[16] Nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ze dne 4. července 2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů (Úř. věst. L 201, 27.7.2012, s. 1).

				2011/24/EU;[17] *6. Dodávky a rozvody pitné vody* dodavatelé a distributoři „vody určené k lidské spotřebě“ ve smyslu čl. 2 bodu 1 písm. a) směrnice Rady 98/83/ES[18], avšak kromě distributorů, pro něž je distribuce vody určené k lidské spotřebě pouze částí jejich obecné činnosti spočívající v distribuci komodit a zboží, která není považována za základní službu *7. Digitální infrastruktura* - výměnné uzly internetu (IXP) - poskytovatelé služeb systému doménových jmen (DNS) registry internetových domén nejvyšší úrovně (TLD)
§ 3 písm. f) až h)	Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou f) správce a provozovatel informačního systému základní služby, pokud nejsou	32016L1148	Čl. 4 odst. 4 a 6	4) „provozovatelem základních služeb“ veřejný nebo soukromý subjekt, jehož druh je uveden v příloze II a jenž splňuje kritéria stanovené v čl. 5 odst. 2; 6) „poskytovatelem digitálních služeb“ jakákoli právnická osoba poskytující digitální

[17] Směrnice Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči (Úř. věst. L 88, 4.4.2011, s. 45).

[18] Směrnice Rady 98/83/ES ze dne 3. listopadu 1998 o jakosti vody určené k lidské spotřebě (Úř. věst. L 330, 5.12.1998, s. 32).

	správcem podle písmene c) nebo d), g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a h) poskytovatel digitální služby.			službu;
§ 3a	§3a Zástupce poskytovatele digitální služby (1) Poskytovatel digitální služby, který poskytuje tuto službu v České republice, nemá sídlo v Evropské unii a neustavil si svého zástupce v jiném členském státě Evropské unie „(dále jen „jiný členský stát“), je povinen ustavit si svého zástupce v České republice. Zástupcem poskytovatele digitální služby je osoba, která je usazená v České republice a která je poskytovatelem digitální služby na základě plné moci zmocněná jej zastupovat ve vztahu k povinnostem podle tohoto zákona. (2) V případě, že poskytovatel digitální služby má sídlo mimo Evropskou unii a ustavil si svého zástupce v České republice, má se za to, že je usazen v České republice a vztahují se na něj povinnosti podle tohoto zákona. (3) V případě, že je poskytovatel digitální služby usazen v České republice nebo zde má ustaveného zástupce, ale jím využívané sítě elektronických komunikací a informační systémy se nacházejí v jiném členském státu, Úřad při výkonu státní správy spolupracuje s příslušným orgánem dotčeného členského	32016L1148	Čl. 17 odst. 3	3. Pokud je poskytovatel digitálních služeb primárně usazen nebo má zástupce v jednom členském státě, ale jeho sítě a informační systémy se nacházejí v jednom či více jiných členských státech, příslušný orgán členského státu, v němž je poskytovatel primárně usazen nebo v němž má svého zástupce, a příslušné orgány těchto jiných členských států podle potřeby spolupracují a jsou si navzájem nápomocny. Taková pomoc a spolupráce může zahrnovat výměny informací mezi dotčenými příslušnými orgány a žádosti o přijetí kontrolních opatření podle odstavce 2.

	státu.		Čl. 4 odst. 10	10) „zástupcem“ fyzická či právnická osoba usazená v Unii, výslovně pověřená, aby jednala jménem poskytovatele digitálních služeb, jenž v Unii usazen není, přičemž vnitrostátní příslušný orgán nebo tým CSIRT může se zástupcem jednat namísto daného poskytovatele digitálních služeb, pokud jde o povinnosti poskytovatele digitálních služeb vyplývající z této směrnice;
			Čl. 18 odst. 1 a 2	1. Pro účely této směrnice se má za to, že poskytovatel digitálních služeb podléhá pravomoci členského státu, v němž je primárně usazen. Má-li poskytovatel digitálních služeb v některém členském státě své sídlo, má se za to, že je v tomto členském státě rovněž primárně usazen. 2. Poskytovatel digitálních služeb, který není v Unii usazen, ale nabízí v Unii služby uvedené v příloze III, určí svého zástupce v Unii. Tento zástupce musí být usazen v jednom ze členských států, v němž jsou služby nabízeny. Má se za to, že poskytovatel digitálních služeb podléhá pravomoci členského státu, v němž je zástupce usazen.
§ 4 odst. 2	**(**2) Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační	32016L1148	Čl. 14 odst. 1 a 2	1. Členské státy zajistí, aby jejich provozovatelé základních služeb přijali vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež provozovatelé používají pro výkon své činnosti. S ohledem na nejnovější

	infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci.			technický vývoj tato opatření musí zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. 2. Členské státy zajistí, aby provozovatelé základních služeb přijali vhodná opatření k předcházení incidentům ovlivňujícím bezpečnost sítí a informačních systémů používaných pro poskytování těchto základních služeb a k minimalizaci jejich dopadu, aby byla zajištěna kontinuita těchto služeb.
			Čl. 1 odst. 2 písm. d)	Za tímto účelem tato směrnice: d) zavádí bezpečnostní požadavky a požadavky na hlášení incidentů pro provozovatele základních služeb a pro poskytovatele digitálních služeb;
§ 4 odst. 3	(3) Poskytovatel digitální služby je povinen zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě a informační systémy, které využívá v souvislosti se zajišťováním své služby, přičemž tato bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy.	32016L1148	Čl. 16 odst. 1 a 2	1. Členské státy zajistí, aby poskytovatelé digitálních služeb určili a přijali vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž jsou vystaveny sítě a informační systémy, které využívají v souvislosti s nabízením služeb uvedených v příloze III v rámci Unie. S ohledem na nejnovější technický vývoj tato opatření musí zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika, přičemž zohledňují: a) bezpečnost systémů a zařízení; b) řešení incidentů; c) řízení kontinuity provozu; d) monitorování, audity a testování;

				e) soulad s mezinárodními normami. 2. Členské státy zajistí, aby poskytovatelé digitálních služeb přijali opatření k předcházení incidentům ovlivňujícím bezpečnost jejich sítí a informačních systémů a k minimalizaci dopadu těchto incidentů na služby uvedené v příloze III, které jsou nabízeny v rámci Unie, aby byla zajištěna kontinuita těchto služeb.
			Čl. 1 odst. 2 písm. d)	Za tímto účelem tato směrnice: d) zavádí bezpečnostní požadavky a požadavky na hlášení incidentů pro provozovatele základních služeb a pro poskytovatele digitálních služeb;
§ 4 odst. 4 a 5	(4) Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži. (5) Orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, jsou povinny si ve smlouvě, kterou uzavírají s poskytovatelem služeb cloud computingu, zajistit alespoň, že jim budou na základě jejich žádosti bez zbytečného odkladu poskytnuty	32016L1148	Čl. 1 odst. 6	6. Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti.

	informace a data, která pro ně poskytovatel služeb cloud computingu uchovává, a bez zbytečného odkladu umožněna jejich kontrola. Nezbytnými náležitostmi smlouvy jsou a) zakotvení povinnosti poskytovatele služeb respektovat bezpečnostní politiky odběratele služeb, b) stanovení úrovně poskytovaných služeb, c) systém schvalování subdodavatelů služby cloud computingu, d) podmínky ukončení smluvního vztahu z pohledu bezpečnosti, e) řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu, f) určení vlastníka uchovávaných dat, g) dohoda o důvěrnosti smluvního vztahu, h) stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity, i) pravidla zákaznického auditu, j) stanovení povinnosti poskytovatele služeb informovat odběratele o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy.			
			Čl. 3	Aniž je dotčen čl. 16 odst. 10 a aniž jsou dotčeny povinnosti členských států podle práva Unie, mohou členské státy přijímat nebo ponechat

				v platnosti ustanovení, jejichž cílem je dosáhnout vyšší úrovně bezpečnosti sítí a informačních systémů.
			Čl. 14 odst. 1 a 2	1. Členské státy zajistí, aby jejich provozovatelé základních služeb přijali vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež provozovatelé používají pro výkon své činnosti. S ohledem na nejnovější technický vývoj tato opatření musí zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. 2. Členské státy zajistí, aby provozovatelé základních služeb přijali vhodná opatření k předcházení incidentům ovlivňujícím bezpečnost sítí a informačních systémů používaných pro poskytování těchto základních služeb a k minimalizaci jejich dopadu, aby byla zajištěna kontinuita těchto služeb.
§ 4a odst. 3	(3) Orgány a osoby, které byly podle § 22a určené provozovateli základní služby a nejsou zároveň správci nebo provozovateli svých informačních systémů základní služby, jsou povinny správce nebo provozovatele tohoto informačního systému základní služby neprodleně a prokazatelně informovat o svém určení a o tom, že se dotčený správce nebo provozovatel stal orgánem nebo osobou podle § 3 písm. f).	32016L1148	Čl. 5 odst. 1	1. Do 9. listopadu 2018 členské státy v každém odvětví a pododvětví uvedeném v příloze II určí provozovatele základních služeb usazené na jejich území.

§ 6	§ 6 Prováděcí právní předpis stanoví a) obsah bezpečnostních opatření, b) obsah a strukturu bezpečnostní dokumentace, c) rozsah bezpečnostních opatření pro orgány a osoby uvedené v § 3 písm. c) až f), d) významné informační systémy a jejich určující kritéria.	32016L1148	Čl. 14 odst. 1 a 2 Čl. 1 odst. 2 písm. d)	1. Členské státy zajistí, aby jejich provozovatelé základních služeb přijali vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež provozovatelé používají pro výkon své činnosti. S ohledem na nejnovější technický vývoj tato opatření musí zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. 2. Členské státy zajistí, aby provozovatelé základních služeb přijali vhodná opatření k předcházení incidentům ovlivňujícím bezpečnost sítí a informačních systémů používaných pro poskytování těchto základních služeb a k minimalizaci jejich dopadu, aby byla zajištěna kontinuita těchto služeb. Za tímto účelem tato směrnice: d) zavádí bezpečnostní požadavky a požadavky na hlášení incidentů pro provozovatele základních služeb a pro poskytovatele digitálních služeb;
§ 7 odst. 3	(3) Orgány a osoby uvedené v § 3 písm. b) až f) jsou povinny detekovat kybernetické bezpečnostní události v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému.	32016L1148	Čl. 14 odst. 2	2. Členské státy zajistí, aby provozovatelé základních služeb přijali vhodná opatření k předcházení incidentům ovlivňujícím bezpečnost sítí a informačních systémů používaných pro poskytování těchto základních služeb a k minimalizaci jejich dopadu, aby byla zajištěna kontinuita těchto služeb.

§ 8 odst. 1	(1) Orgány a osoby uvedené v § 3 písm. b) až f) jsou povinny hlásit kybernetické bezpečnostní incidenty v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému, a to bezodkladně po jejich detekci; tím není dotčena informační povinnost podle jiného právního předpisu[3)] nebo přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů[11)]. V případě, že kybernetický bezpečnostní incident má významný dopad na kontinuitu poskytování základní služby, oznámí to provozovatel základní služby Úřadu. _____ 11) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).	32016L1148	Čl. 14 odst. 3 a 4	3. Členské státy zajistí, aby provozovatelé základních služeb hlásili příslušnému orgánu nebo týmu CSIRT bez zbytečného prodlení incidenty se závažným dopadem na kontinuitu základních služeb, které poskytují. Hlášení zahrnuje informace, které příslušnému orgánu nebo týmu CSIRT umožní posoudit případný přeshraniční dopad daného incidentu. Ohlášení nezakládá u oznamující strany vyšší míru právní odpovědnosti. 4. Při posuzování významnosti dopadu incidentu se zohlední zejména tyto parametry: a) počet uživatelů postižených narušením základní služby; b) délka trvání incidentu; c) zeměpisný rozsah oblasti dotčené incidentem.
			Čl. 1 odst. 2 písm. d)	Za tímto účelem tato směrnice: d) zavádí bezpečnostní požadavky a požadavky na hlášení incidentů pro provozovatele základních služeb a pro poskytovatele digitálních služeb;
		32016R0679	Čl. 33	1. Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno

				do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění. 2. Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci. 3. Ohlášení podle odstavce 1 musí přinejmenším obsahovat: a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů; b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace; c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů; d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů. 4. Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu. 5. Správce dokumentuje veškeré případy porušení

				zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.
§ 8 odst. 2	(2) Poskytovatel digitální služby je povinen bez zbytečného odkladu hlásit kybernetický bezpečnostní incident s významným dopadem na poskytování jeho služeb, pokud má přístup k informacím nezbytným pro posouzení významnosti tohoto dopadu.	32016L1148	Čl. 16 odst. 3 a 4	3. Členské státy zajistí, aby poskytovatelé digitálních služeb bez zbytečného odkladu hlásili příslušnému orgánu nebo týmu CSIRT incidenty, které mají významný dopad na poskytování služby uvedené v příloze III, kterou nabízejí v rámci Unie. Hlášení musí obsahovat takové informace, které příslušnému orgánu nebo týmu CSIRT umožní posoudit významnost případného přeshraničního dopadu daného incidentu. Ohlášení nezakládá u oznamující strany vyšší míru právní odpovědnosti. 4. Při posuzování toho, zda je dopad incidentu významný, se zohlední zejména tyto parametry: a) počet uživatelů postižených incidentem, zejména těch uživatelů, kteří na službu spoléhají při poskytování vlastních služeb; b) délka trvání incidentu; c) zeměpisný rozsah oblasti dotčené incidentem; d) rozsah, v jakém bylo narušeno fungování služby; e) rozsah dopadu na společenské a ekonomické činnosti. Ohlášení incidentu je povinné, pouze pokud má poskytovatel digitální služby přístup k informacím,

				které jsou nezbytné k posouzení dopadu incidentu na základě parametrů uvedených v prvním pododstavci.
			Čl. 1 odst. 2 písm. d)	Za tímto účelem tato směrnice: d) zavádí bezpečnostní požadavky a požadavky na hlášení incidentů pro provozovatele základních služeb a pro poskytovatele digitálních služeb;
§ 8 odst. 3 až 5	(3) Orgány a osoby uvedené v § 3 písm. b) a h) hlásí kybernetické bezpečnostní incidenty provozovateli národního CERT. (4) Orgány a osoby uvedené v § 3 písm. c) až g) hlásí kybernetické bezpečnostní incidenty Úřadu. (5) Orgány a osoby neuvedené v § 3 mohou hlásit kybernetické bezpečnostní incidenty provozovateli národního CERT, nebo Úřadu.	32016L1148	Čl. 14 odst. 3	3. Členské státy zajistí, aby provozovatelé základních služeb hlásili příslušnému orgánu nebo týmu CSIRT bez zbytečného prodlení incidenty se závažným dopadem na kontinuitu základních služeb, které poskytují. Hlášení zahrnuje informace, které příslušnému orgánu nebo týmu CSIRT umožní posoudit případný přeshraniční dopad daného incidentu. Ohlášení nezakládá u oznamující strany vyšší míru právní odpovědnosti.
			Čl. 16 odst. 3	3. Členské státy zajistí, aby poskytovatelé digitálních služeb bez zbytečného odkladu hlásili příslušnému orgánu nebo týmu CSIRT incidenty, které mají významný dopad na poskytování služby uvedené v příloze III, kterou nabízejí v rámci Unie. Hlášení musí obsahovat takové informace, které příslušnému orgánu nebo týmu CSIRT umožní posoudit významnost případného přeshraničního dopadu daného incidentu. Ohlášení nezakládá u oznamující strany vyšší míru právní odpovědnosti.

			Čl. 20 odst. 2	Při zpracování hlášení postupují členské státy postupem stanoveným v článku 14. Členské státy mohou dát přednost zpracování povinných hlášení před dobrovolnými hlášeními. Dobrovolná hlášení se zpracují pouze za podmínky, že jejich zpracování nepředstavuje pro dotčené členské státy nepřiměřenou nebo nepatřičnou zátěž. Na základě dobrovolného ohlášení nesmí být oznamujícímu subjektu uložena žádná povinnost, která by mu nebyla uložena, kdyby toto ohlášení neučinil.
§ 8 odst. 6 písm. a)	Prováděcí právní předpis stanoví a) typy, kategorie a hodnocení významnosti dopadu kybernetického bezpečnostního incidentu a	32016L1148	Čl. 14 odst. 4	4. Při posuzování významnosti dopadu incidentu se zohlední zejména tyto parametry: a) počet uživatelů postižených narušením základní služby; b) délka trvání incidentu; c) zeměpisný rozsah oblasti dotčené incidentem.
			Čl. 16 odst. 4	4. Při posuzování toho, zda je dopad incidentu významný, se zohlední zejména tyto parametry: a) počet uživatelů postižených incidentem, zejména těch uživatelů, kteří na službu spoléhají při poskytování vlastních služeb; b) délka trvání incidentu; c) zeměpisný rozsah oblasti dotčené incidentem; d) rozsah, v jakém bylo narušeno fungování

				služby; e) rozsah dopadu na společenské a ekonomické činnosti. Ohlášení incidentu je povinné, pouze pokud má poskytovatel digitální služby přístup k informacím, které jsou nezbytné k posouzení dopadu incidentu na základě parametrů uvedených v prvním pododstavci.
			Čl. 20 odst. 2	Při zpracování hlášení postupují členské státy postupem stanoveným v článku 14. Členské státy mohou dát přednost zpracování povinných hlášení před dobrovolnými hlášeními. Dobrovolná hlášení se zpracují pouze za podmínky, že jejich zpracování nepředstavuje pro dotčené členské státy nepřiměřenou nebo nepatřičnou zátěž. Na základě dobrovolného ohlášení nesmí být oznamujícímu subjektu uložena žádná povinnost, která by mu nebyla uložena, kdyby toto ohlášení neučinil.
§ 8 odst. 7	(7) Pokud má kybernetický bezpečnostní incident, který postihnul poskytovatele digitální služby, významný dopad na kontinuitu poskytování základní služby, je její provozovatel povinen tuto skutečnost Úřadu nahlásit.	32016L1148	čl. 16 odst. 5	5. Pokud provozovatel základních služeb spoléhá na vnějšího poskytovatele digitálních služeb při poskytování služby, která je základní z hlediska zachování kritických společenských a ekonomických činností, ohlásí provozovatel základních služeb jakýkoli významný dopad na kontinuitu těchto základních služeb způsobený incidentem, jímž byl poskytovatel digitálních služeb postižen.
§ 9 odst. 2	(2) Součástí evidence incidentů jsou údaje	32016L1148	Čl. 20	1. Aniž je dotčen článek 3, mohou subjekty, které nebyly určeny jako provozovatelé základních

	podle § 20 písm. f) až h) a l).			služeb a které nejsou poskytovateli digitálních služeb, dobrovolně hlásit incidenty se závažným dopadem na kontinuitu služeb, které poskytují. 2. Při zpracování hlášení postupují členské státy postupem stanoveným v článku 14. Členské státy mohou dát přednost zpracování povinných hlášení před dobrovolnými hlášeními. Dobrovolná hlášení se zpracují pouze za podmínky, že jejich zpracování nepředstavuje pro dotčené členské státy nepřiměřenou nebo nepatřičnou zátěž. Na základě dobrovolného ohlášení nesmí být oznamujícímu subjektu uložena žádná povinnost, která by mu nebyla uložena, kdyby toto ohlášení neučinil.
§ 10a	§ 10a Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila, se podle předpisů upravujících svobodný přístup k informacím neposkytují.	32016L1148	Čl. 1 odst. 6 Čl. 3	6. Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti. Aniž je dotčen čl. 16 odst. 10 a aniž jsou dotčeny povinnosti členských států podle práva Unie, mohou členské státy přijímat nebo ponechat v platnosti ustanovení, jejichž cílem je dosáhnout vyšší úrovně bezpečnosti sítí a informačních systémů.

§ 11 odst. 3 a 4	(3) Reaktivní opatření jsou povinny provádět a) orgány a osoby uvedené v § 3 písm. a) a b) za stavu kybernetického nebezpečí nebo za nouzového stavu[4)] vyhlášeného na základě žádosti podle § 21 odst. 6 a b) orgány a osoby uvedené v § 3 písm. c) až f). (4) Ochranné opatření jsou povinny provádět orgány a osoby uvedené v § 3 písm. c) až f).	32016L1148	Čl. 1 odst. 6 Čl. 3	6. Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti. Aniž je dotčen čl. 16 odst. 10 a aniž jsou dotčeny povinnosti členských států podle práva Unie, mohou členské státy přijímat nebo ponechat v platnosti ustanovení, jejichž cílem je dosáhnout vyšší úrovně bezpečnosti sítí a informačních systémů.
§ 12 odst. 3	(3) Úřad je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn po konzultaci s orgánem nebo osobou uvedenými v § 3 písm. c), d), f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, veřejnost o tomto incidentu informovat nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám. .	32016L1148	Čl. 16 odst. 7	7. V případě, že informovanost veřejnosti je nezbytná pro předejití incidentu nebo ke zvládání probíhajícího incidentu, nebo pokud je zveřejnění incidentu ve veřejném zájmu z jiných důvodů, může příslušný orgán nebo tým CSIRT, jimž byl incident ohlášen, popřípadě příslušný orgán nebo tým CSIRT jiných dotčených členských států po konzultaci dotčeného poskytovatele digitálních služeb informovat o jednotlivých incidentech veřejnost nebo nařídit poskytovateli digitálních služeb, aby tak učinil.

			Čl. 14 odst. 6	Pokud je pro zamezení incidentu nebo zvládání probíhajícího incidentu nezbytná informovanost veřejnosti, může příslušný orgán nebo tým CSIRT po konzultaci ohlašujícího provozovatele základních služeb informovat o jednotlivých incidentech veřejnost.
§ 13 odst. 4	(4) Orgány a osoby uvedené v § 3 písm. a) až f) jsou povinny bez zbytečného odkladu oznámit Úřadu provedení reaktivního opatření a jeho výsledek. Náležitosti oznámení stanoví prováděcí právní předpis.	32016L1148	Čl. 1 odst. 6 Čl. 3	6. Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti. Aniž je dotčen čl. 16 odst. 10 a aniž jsou dotčeny povinnosti členských států podle práva Unie, mohou členské státy přijímat nebo ponechat v platnosti ustanovení, jejichž cílem je dosáhnout vyšší úrovně bezpečnosti sítí a informačních systémů.
§ 16 odst. 2 a 3	(2) Kontaktní údaje a jejich změny oznamují a) orgány a osoby uvedené v § 3 písm. a), b) a h) provozovateli národního CERT a b) orgány a osoby uvedené v § 3 písm. c) až g) Úřadu. (3) Orgány a osoby uvedené § 3 písm. c) až g)	32016L1148	Čl. 15 odst. 2	2. Členské státy zajistí, aby příslušné orgány měly pravomoci a prostředky nezbytné k tomu, aby mohly od provozovatelů základních služeb požadovat poskytnutí: a) informací nezbytných pro posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky;

	oznamují změny pouze těch údajů podle odstavce 1, které nejsou referenčními údaji vedenými v základních registrech, a to neprodleně.			b) dokladů o účinném provádění bezpečnostních politik, jako jsou výsledky bezpečnostního auditu provedeného příslušným orgánem nebo kvalifikovaným auditorem, a v případě kvalifikovaného auditora, aby mohlo být požadováno předložení těchto výsledků včetně podpůrných dokladů příslušnému orgánu. Pokud příslušný orgán žádá o poskytnutí těchto informací nebo dokladů, uvede účel své žádosti a upřesní informace, které jsou požadovány.
			Čl. 17 odst. 2	2. Pro účely odstavce 1 musí mít příslušné orgány nezbytné pravomoci a prostředky, aby mohly od poskytovatelů digitálních služeb požadovat: a) poskytnutí informací potřebných k posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky; b) nápravu případného neplnění požadavků stanovených v článku 16.
			Čl. 1 odst. 6	6. Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti.

§ 16 odst. 6	Úřad je dále oprávněn si pro účely kontroly vyžádat od provozovatele národního CERT kontaktní údaje orgánů a osob uvedených v § 3 písm. h).	32016L1148	Čl. 17 odst. 2 Čl. 1 odst. 6	2. Pro účely odstavce 1 musí mít příslušné orgány nezbytné pravomoci a prostředky, aby mohly od poskytovatelů digitálních služeb požadovat: a) poskytnutí informací potřebných k posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky; b) nápravu případného neplnění požadavků stanovených v článku 16. 6. Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti.
§ 17 odst. 2	(2) Provozovatel národního CERT a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. a), b) a h) a tyto údaje eviduje a uchovává, b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. b) a h) a tyto údaje eviduje, uchovává a chrání, c) vyhodnocuje kybernetické bezpečnostní incidenty u orgánů a osob uvedených v § 3 písm. b) a h),	32016L1148	Čl. 9 odst. 1	1. Každý členský stát zřídí jeden nebo více bezpečnostních týmů typu CSIRT (Computer Security Incident Response Team; dále jen „tým CSIRT“), které pokrývají alespoň odvětví uvedená v příloze II a služby uvedené v příloze III, které jsou odpovědné za zvládání rizik a řešení incidentů podle řádně vymezených postupů a splňují požadavky uvedené v příloze I bodě 1. Tým CSIRT může být zřízen v rámci příslušného orgánu.

	d) poskytuje orgánům a osobám uvedeným v § 3 písm. a), b) a h) metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu, e) působí jako kontaktní místo pro orgány a osoby uvedené v § 3 písm. a), b) a h), f) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti, g) předává Úřadu údaje o kybernetických bezpečnostních incidentech ohlášených podle § 8 odst. 3 bez uvedení ohlašovatele, h) předává Úřadu na vyžádání údaje podle § 16 odst. 5 a 6, i) plní roli týmu CSIRT podle příslušného předpisu Evropské unie[12)], j) informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu s významným dopadem na kontinuitu poskytování základní nebo digitální služby v tomto členském státě a zároveň o tom informuje Úřad, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele, k) spolupracuje s týmy CSIRT jiných členských států a l) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob neuvedených v § 3, a pokud to jeho kapacity umožňují, zpracovává je a poskytuje orgánům nebo osobám dotčeným kybernetickým			

	bezpečnostním incidentem metodickou podporu, pomoc a součinnost. 12) Článek 9 směrnice 2016/1148.		Čl. 9 odst. 2 pododstavec 2	Členské státy zajistí, aby jejich týmy CSIRT v rámci sítě CSIRT uvedené v článku 12 účelně, účinně a spolehlivě spolupracovaly.
			Čl. 1 odst. 2 písm. c) a e)	Za tímto účelem tato směrnice: c) ustavuje síť bezpečnostních týmů typu CSIRT (dále jen „síť CSIRT“), jejímž účelem je přispívat k budování důvěry mezi členskými státy a podporovat rychlou a účinnou operativní spolupráci; e) ukládá členským státům povinnost určit vnitrostátní příslušné orgány, jednotná kontaktní místa a týmy CSIRT, jejichž úkoly budou souviset s bezpečností sítí a informačních systémů.
			Čl. 16 odst. 3 a 6	3. Členské státy zajistí, aby poskytovatelé digitálních služeb bez zbytečného odkladu hlásili příslušnému orgánu nebo týmu CSIRT incidenty, které mají významný dopad na poskytování služby uvedené v příloze III, kterou nabízejí v rámci Unie. Hlášení musí obsahovat takové informace, které příslušnému orgánu nebo týmu CSIRT umožní posoudit významnost případného přeshraničního dopadu daného incidentu. Ohlášení nezakládá u oznamující strany vyšší míru právní odpovědnosti. 6. Tam, kde je to vhodné, a zejména pokud se

				incident podle odstavce 3 týká dvou nebo více členských států, informuje příslušný orgán nebo tým CSIRT, jimž byl incident ohlášen, ostatní dotčené členské státy. Příslušné orgány, týmy CSIRT a jednotná kontaktní místa přitom v souladu s právem Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zachovávají bezpečnost a obchodní zájmy poskytovatele digitálních služeb, jakož i důvěrnost poskytnutých informací.
			Čl. 10 odst. 1 a 2	1. Pokud existují odděleně, příslušný orgán, jednotné kontaktní místo a týmy CSIRT téhož členského státu vzájemně spolupracují při plnění povinností stanovených touto směrnicí. 2. Členské státy zajistí, aby příslušné orgány nebo týmy CSIRT obdržely hlášení o incidentech podaná podle této směrnice. Pokud členský stát rozhodne, že týmy CSIRT nemají hlášení přijímat, bude týmům CSIRT v rozsahu nezbytném pro plnění jejich úkolů povolen přístup k údajům o incidentech hlášených provozovateli základních služeb podle čl. 14 odst. 3 a 5 nebo poskytovateli digitálních služeb podle čl. 16 odst. 3 a 6.
			Čl. 10 odst. 3 první pododstavec	3. Členské státy zajistí, aby příslušné orgány nebo týmy CSIRT informovaly jednotná kontaktní místa o hlášeních incidentů podaných podle této směrnice.

			Čl. 12 odst. 2	2. Síť CSIRT tvoří zástupci týmů CSIRT z členských států a týmu CERT-EU. Komise se účastní sítě CSIRT jako pozorovatel. Agentura ENISA zajistí služby sekretariátu a aktivně podporuje spolupráci mezi týmy CSIRT.
			Čl. 20	1. Aniž je dotčen článek 3, mohou subjekty, které nebyly určeny jako provozovatelé základních služeb a které nejsou poskytovateli digitálních služeb, dobrovolně hlásit incidenty se závažným dopadem na kontinuitu služeb, které poskytují. 2. Při zpracování hlášení postupují členské státy postupem stanoveným v článku 14. Členské státy mohou dát přednost zpracování povinných hlášení před dobrovolnými hlášeními. Dobrovolná hlášení se zpracují pouze za podmínky, že jejich zpracování nepředstavuje pro dotčené členské státy nepřiměřenou nebo nepatřičnou zátěž. Na základě dobrovolného ohlášení nesmí být oznamujícímu subjektu uložena žádná povinnost, která by mu nebyla uložena, kdyby toto ohlášení neučinil.
			Příloha I odst. 2	2) Úkoly týmů CSIRT a) Úkoly týmů CSIRT zahrnují alespoň: i) monitorování incidentů na vnitrostátní úrovni; ii) vydávání včasných varování a upozornění, oznamování a šíření informací o rizicích a incidentech příslušným zúčastněným stranám;

				iii) reakce na incidenty; iv) poskytování dynamické analýzy rizik a incidentů a přehledu o situaci, v) účast v síti CSIRT. b) Týmy CSIRT naváží spolupráci se soukromým sektorem. c) V zájmu usnadnění spolupráce týmy CSIRT prosazují přijetí a používání společných či standardních postupů v oblasti: i) řešení incidentů a rizik; ii) klasifikace incidentů, rizik a informací.
§ 18 odst. 5	Provozovatel národního CERT je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v § 17 odst. 2 nezbytné náklady.	32016L1148	Čl. 9 odst. 2 pododstavec 1	Členské státy zajistí, aby týmy CSIRT měly odpovídající zdroje pro účinné plnění jejich úkolů podle přílohy I bodu 2.
§ 20	Vládní CERT jako součást Úřadu a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. c) až g), b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. c) až g), c) vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech z kritické informační infrastruktury, informačního systému základní služby, významných informačních systémů a dalších informačních	32016L1148	Čl. 9 odst. 1	1. Každý členský stát zřídí jeden nebo více bezpečnostních týmů typu CSIRT (Computer Security Incident Response Team; dále jen „tým CSIRT“), které pokrývají alespoň odvětví uvedená v příloze II a služby uvedené v příloze III, které jsou odpovědné za zvládání rizik a řešení incidentů podle řádně vymezených postupů a splňují požadavky uvedené v příloze I bodě 1. Tým CSIRT může být zřízen v rámci příslušného orgánu.

	systémů veřejné správy, d) poskytuje orgánům a osobám uvedeným v § 3 písm. c) až g) metodickou podporu a pomoc, e) poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až g) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události, f) přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje, g) přijímá údaje od provozovatele národního CERT a tyto údaje vyhodnocuje, h) přijímá údaje od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, a tyto údaje vyhodnocuje, i) poskytuje podle § 9 odst. 4 provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti údaje z evidence incidentů, j) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti, k) informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu, který má významný dopad na kontinuitu poskytování základních služeb v tomto členském státě nebo se dotýká			

	poskytování digitálních služeb v tomto členském státě, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele, l) přijímá hlášení o kybernetickém bezpečnostním incidentu od orgánů a osob neuvedených v § 3; vládní CERT hlášení zpracovává, a pokud to jeho kapacity umožňují a jedná se o kybernetický bezpečnostní incident s významným dopadem, poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost, m) plní roli týmu CSIRT podle příslušného předpisu Evropské unie[12)],a n) spolupracuje s týmy CSIRT jiných členských států. 12) Článek 9 směrnice 2016/1148.			
			Čl. 1 odst. 2 písm. c) a e)	Za tímto účelem tato směrnice: c) ustavuje síť bezpečnostních týmů typu CSIRT (dále jen „síť CSIRT“), jejímž účelem je přispívat k budování důvěry mezi členskými státy a podporovat rychlou a účinnou operativní spolupráci; e) ukládá členským státům povinnost určit vnitrostátní příslušné orgány, jednotná kontaktní místa a týmy CSIRT, jejichž úkoly budou souviset s

				bezpečností sítí a informačních systémů.
			Čl. 9 odst. 2 pododstavec 2	Členské státy zajistí, aby jejich týmy CSIRT v rámci sítě CSIRT uvedené v článku 12 účelně, účinně a spolehlivě spolupracovaly.
			Čl. 10 odst. 1 a 2	1. Pokud existují odděleně, příslušný orgán, jednotné kontaktní místo a týmy CSIRT téhož členského státu vzájemně spolupracují při plnění povinností stanovených touto směrnicí. 2. Členské státy zajistí, aby příslušné orgány nebo týmy CSIRT obdržely hlášení o incidentech podaná podle této směrnice. Pokud členský stát rozhodne, že týmy CSIRT nemají hlášení přijímat, bude týmům CSIRT v rozsahu nezbytném pro plnění jejich úkolů povolen přístup k údajům o incidentech hlášených provozovateli základních služeb podle čl. 14 odst. 3 a 5 nebo poskytovateli digitálních služeb podle čl. 16 odst. 3 a 6.
			Čl. 12 odst. 2	2. Síť CSIRT tvoří zástupci týmů CSIRT z členských států a týmu CERT-EU. Komise se účastní sítě CSIRT jako pozorovatel. Agentura ENISA zajistí služby sekretariátu a aktivně podporuje spolupráci mezi týmy CSIRT.
			Čl. 14 odst. 3 až 5	3. Členské státy zajistí, aby provozovatelé základních služeb hlásili příslušnému orgánu nebo týmu CSIRT bez zbytečného prodlení incidenty se závažným dopadem na kontinuitu základních služeb, které poskytují. Hlášení zahrnuje informace, které příslušnému orgánu nebo týmu

				CSIRT umožní posoudit případný přeshraniční dopad daného incidentu. Ohlášení nezakládá u oznamující strany vyšší míru právní odpovědnosti. 4. Při posuzování významnosti dopadu incidentu se zohlední zejména tyto parametry: a) počet uživatelů postižených narušením základní služby; b) délka trvání incidentu; c) zeměpisný rozsah oblasti dotčené incidentem. 5. Na základě informací, které provozovatel základních služeb poskytl v hlášení, informuje příslušný orgán nebo tým CSIRT další dotčený členský stát nebo dotčené členské státy, pokud má incident významný dopad na kontinuitu základních služeb v tomto členském státě nebo členských státech. Příslušný orgán nebo tým CSIRT přitom v souladu s právem Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zachová bezpečnost a obchodní zájmy provozovatele základních služeb, jakož i důvěrnost informací poskytnutých v jeho hlášení. Pokud to okolnosti dovolují, příslušný orgán nebo tým CSIRT poskytne ohlašujícímu provozovateli základních služeb relevantní informace týkající se následných opatření přijatých na základě jeho hlášení, například informace, které by mohly podpořit účinné řešení incidentu. Na žádost příslušného orgánu nebo týmu CSIRT

				postoupí jednotné kontaktní místo hlášení uvedená v prvním pododstavci jednotným kontaktním místům dalších dotčených členských států.
			Čl. 16 odst. 6	6. Tam, kde je to vhodné, a zejména pokud se incident podle odstavce 3 týká dvou nebo více členských států, informuje příslušný orgán nebo tým CSIRT, jimž byl incident ohlášen, ostatní dotčené členské státy. Příslušné orgány, týmy CSIRT a jednotná kontaktní místa přitom v souladu s právem Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zachovávají bezpečnost a obchodní zájmy poskytovatele digitálních služeb, jakož i důvěrnost poskytnutých informací.
			Čl. 20	1. Aniž je dotčen článek 3, mohou subjekty, které nebyly určeny jako provozovatelé základních služeb a které nejsou poskytovateli digitálních služeb, dobrovolně hlásit incidenty se závažným dopadem na kontinuitu služeb, které poskytují. 2. Při zpracování hlášení postupují členské státy postupem stanoveným v článku 14. Členské státy mohou dát přednost zpracování povinných hlášení před dobrovolnými hlášeními. Dobrovolná hlášení se zpracují pouze za podmínky, že jejich zpracování nepředstavuje pro dotčené členské státy nepřiměřenou nebo nepatřičnou zátěž. Na základě dobrovolného ohlášení nesmí být oznamujícímu subjektu uložena žádná povinnost, která by mu nebyla uložena, kdyby toto ohlášení

				neučinil.
			Příloha I odst. 2	2) Úkoly týmů CSIRT a) Úkoly týmů CSIRT zahrnují alespoň: i) monitorování incidentů na vnitrostátní úrovni; ii) vydávání včasných varování a upozornění, oznamování a šíření informací o rizicích a incidentech příslušným zúčastněným stranám; iii) reakce na incidenty; iv) poskytování dynamické analýzy rizik a incidentů a přehledu o situaci, v) účast v síti CSIRT. b) Týmy CSIRT naváží spolupráci se soukromým sektorem. c) V zájmu usnadnění spolupráce týmy CSIRT prosazují přijetí a používání společných či standardních postupů v oblasti: i) řešení incidentů a rizik; ii) klasifikace incidentů, rizik a informací.

§ 22 odst. 2	(2) Úřad a) stanoví bezpečnostní opatření, b) vydává opatření, c) zajišťuje činnost Národního centra kybernetické bezpečnosti, d) vede evidence podle tohoto zákona, e) ukládá pokuty za správní delikty podle tohoto zákona, f) působí jako koordinační orgán ve stavu kybernetického nebezpečí, g) spolupracuje s orgány a osobami, které působí v oblasti kybernetické bezpečnosti, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT, h) zajišťuje mezinárodní spolupráci, i) sjednává a uzavírá smlouvy o mezinárodní spolupráci, j) zajišťuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti, k) zajišťuje výzkum a vývoj v oblasti kybernetické bezpečnosti, l) uzavírá veřejnoprávní smlouvu s provozovatelem národního CERT, m) zasílá podle krizového zákona Ministerstvu vnitra návrh prvků kritické infrastruktury v odvětví komunikační a informační systémy v	32016L1148	Čl. 5 odst. 1, 5 a 7	1. Do 9. listopadu 2018 členské státy v každém odvětví a pododvětví uvedeném v příloze II určí provozovatele základních služeb usazené na jejich území. 5. Seznam určených provozovatelů základních služeb členské státy pravidelně, a to alespoň každé dva roky ode dne 9. května 2018, přezkoumávají a v případě potřeby jej aktualizují. 7. Pro účely přezkumu uvedeného v článku 23 členské státy do 9. listopadu 2018 a poté každé dva roky předkládají Komisi informace, jež Komise potřebuje k hodnocení provádění této směrnice, zejména z hlediska konzistentnosti přístupů členských států v otázce určování provozovatelů základních služeb. Tyto informace zahrnují alespoň: a) vnitrostátní opatření umožňující určení provozovatelů základních služeb; b) seznam služeb uvedený v odstavci 3; c) počet provozovatelů základních služeb určených v každém odvětví podle přílohy II a jejich význam ve vztahu k dotyčnému odvětví; d) mezní hodnoty, existují-li, pro stanovení příslušné zásobovací úrovně podle počtu uživatelů závislých na dané službě podle čl. 6 odst. 1 písm. a) nebo významu konkrétního provozovatele základních služeb podle čl. 6 odst. 1 písm. f). V zájmu větší srovnatelnosti poskytovaných informací může Komise s maximálním ohledem na stanovisko agentury ENISA přijmout patřičné

	oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu, n) určuje podle krizového zákona prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, pokud nejde o prvky uvedené v písmeni m), o) každé 2 roky ověřuje aktuálnost určení prvků kritické infrastruktury podle písmen m) a n), p) určuje provozovatele základní služby a informační systém základní služby, q) zpracovává a vládě ke schválení předkládá národní strategii kybernetické bezpečnosti[13)] a akční plán k jejímu naplňování a tuto strategii aktualizuje nejméně každých 5 let, r) je jednotným kontaktním místem pro zajištění přeshraniční spolupráce v rámci Evropské unie, s) je příslušným orgánem v České republice a plní informační povinnosti vůči Evropské komisi a skupině pro spolupráci podle příslušného předpisu Evropské unie[14)]. t) informuje veřejnost o kybernetickém bezpečnostním incidentu podle § 12 odst. 3, u) provádí analýzu a monitoring kybernetických hrozeb a rizik a v)plní další úkoly v oblasti kybernetické bezpečnosti stanovené tímto zákonem.			technické pokyny upravující parametry informací uvedených v tomto odstavci.

	13) Čl. 7 směrnice Evropského parlamentu a Rady (EU) 2016/1148. 14) Například čl. 5 odst. 3, čl. 7 odst. 3 a čl. 8 směrnice Evropského parlamentu a Rady (EU) 2016/1148.			

			Čl. 1 odst. 2 písm. a) a e)	Za tímto účelem tato směrnice: a) ukládá všem členským státům povinnost přijmout národní strategii pro bezpečnost sítí a informačních systémů; e) ukládá členským státům povinnost určit vnitrostátní příslušné orgány, jednotná kontaktní místa a týmy CSIRT, jejichž úkoly budou souviset s bezpečností sítí a informačních systémů.
			Čl. 7 odst. 1 a 3	1. Každý členský stát přijme národní strategii pro bezpečnost sítí a informačních systémů, ve které vymezí strategické cíle a příslušná politická a regulační opatření s cílem dosáhnout vysoké úrovně bezpečnosti sítí a informačních systémů a udržovat ji a která pokrývá alespoň odvětví uvedená v příloze II a služby uvedené v příloze III. Předmětem národní strategie pro bezpečnost sítí a informačních systémů jsou především následující cíle a opatření: a) cíle a priority národní strategie pro bezpečnost sítí a informačních systémů; b) správní rámec pro naplnění cílů a priorit vnitrostátní strategie pro bezpečnost sítí a informačních systémů, včetně úlohy a povinností vládních orgánů a dalších relevantních subjektů; c) stanovení opatření týkajících se připravenosti, reakce a obnovy, včetně spolupráce veřejného a soukromého sektoru; d) vymezení vzdělávacích, informačních a

				školicích programů souvisejících s vnitrostátní strategií pro bezpečnost sítí a informačních systémů; e) vymezení výzkumných a rozvojových plánů souvisejících s národní strategií pro bezpečnost sítí a informačních systémů; f) plán posouzení rizik pro určení rizik; g) seznam různých subjektů zapojených do provádění národní strategie pro bezpečnost sítí a informačních systémů. 3. Členské státy oznámí své národní strategie pro bezpečnost sítí a informačních systémů Komisi do tří měsíců od jejich přijetí. Členské státy mohou z oznámení vyloučit prvky strategie, které souvisejí s národní bezpečností.
			Čl. 8 odst. 1 až 4 a 7	1. Každý členský stát určí jeden nebo více vnitrostátních příslušných orgánů v oblasti bezpečnosti sítí a informačních systémů (dále jen „příslušný orgán“) alespoň pro odvětví podle přílohy II a služby podle přílohy III. Členské státy mohou tuto úlohu svěřit již existujícímu orgánu nebo orgánům. 2. Příslušné orgány dohlížejí na provádění této směrnice na vnitrostátní úrovni. 3. Každý členský stát určí vnitrostátní jednotné kontaktní místo pro oblast bezpečnosti sítí a informačních systémů (dále jen „jednotné kontaktní místo“). Členské státy mohou tuto úlohu svěřit již existujícímu orgánu . Určí-li členský

				stát pouze jeden příslušný orgán, je tento orgán rovněž jednotným kontaktním místem. 4. Jednotné kontaktní místo plní styčnou funkci s cílem zajistit přeshraniční spolupráci orgánů členských států s relevantními orgány v jiných členských státech a se skupinou pro spolupráci uvedenou v článku 11 a sítí CSIRT uvedenou v článku 12. 7. Každý členský stát Komisi neprodleně oznámí určení příslušného orgánu a jednotného kontaktního místa, jejich úkoly a jakékoliv změny, které se jich týkají. Každý členský stát zveřejní určení příslušného orgánu a jednotného kontaktního místa. Komise zveřejní seznam určených jednotných kontaktních míst.
			Čl. 9 odst. 4	4. Členské státy oznámí Komisi oblast působnosti svých týmů CSIRT, jakož i hlavní prvky jejich postupu při řešení incidentů.
			Čl. 10 odst. 3	3. Členské státy zajistí, aby příslušné orgány nebo týmy CSIRT informovaly jednotná kontaktní místa o hlášeních incidentů podaných podle této směrnice. Do dne 9. srpna 2018 a poté každý rok předloží jednotné kontaktní místo skupině pro spolupráci souhrnnou zprávu o obdržených hlášeních včetně jejich počtu a povahy ohlášených incidentů, jakož i přijatých opatření ve smyslu čl. 14 odst. 3 a 5 a čl. 16 odst. 3 a 6.

			Čl. 14 odst. 5 druhý a třetí pododstavec	Pokud to okolnosti dovolují, příslušný orgán nebo tým CSIRT poskytne ohlašujícímu provozovateli základních služeb relevantní informace tkající se následných opatření přijatých na základě jeho hlášení, například informace, které by mohly podpořit účinné řešení incidentu. Na žádost příslušného orgánu nebo týmu CSIRT postoupí jednotné kontaktní místo hlášení uvedená v prvním pododstavci jednotným kontaktním místům dalších dotčených členských států.
			Čl. 15 odst. 1 a 2	1. Členské státy zajistí, aby příslušné orgány měly všechny nezbytné pravomoci a prostředky pro posouzení toho, zda provozovatelé základních služeb dodržují své povinnosti podle článku 14, a s tím souvisejících důsledků pro bezpečnost sítí a informačních systémů. 2. Členské státy zajistí, aby příslušné orgány měly pravomoci a prostředky nezbytné k tomu, aby mohly od provozovatelů základních služeb požadovat poskytnutí: a) informací nezbytných pro posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky; b) dokladů o účinném provádění bezpečnostních politik, jako jsou výsledky bezpečnostního auditu provedeného příslušným orgánem nebo kvalifikovaným auditorem, a v případě kvalifikovaného auditora, aby mohlo být

				požadováno předložení těchto výsledků včetně podpůrných dokladů příslušnému orgánu. Pokud příslušný orgán žádá o poskytnutí těchto informací nebo dokladů, uvede účel své žádosti a upřesní informace, které jsou požadovány.
			Čl. 17	1. Členské státy zajistí, aby příslušné orgány v případě potřeby přijaly opatření v rámci následné kontroly, mají-li důkazy o tom, že poskytovatel digitálních služeb nesplňuje požadavky stanovené v článku 16. Takové důkazy mohou být předloženy příslušným orgánem jiného členského státu, v němž je služba poskytována. 2. Pro účely odstavce 1 musí mít příslušné orgány nezbytné pravomoci a prostředky, aby mohly od poskytovatelů digitálních služeb požadovat: a) poskytnutí informací potřebných k posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky; b) nápravu případného neplnění požadavků stanovených v článku 16. 3. Pokud je poskytovatel digitálních služeb primárně usazen nebo má zástupce v jednom členském státě, ale jeho sítě a informační systémy se nacházejí v jednom či více jiných členských státech, příslušný orgán členského státu, v němž je poskytovatel primárně usazen nebo v němž má svého zástupce, a příslušné orgány těchto jiných členských států podle potřeby spolupracují a jsou

				si navzájem nápomocny. Taková pomoc a spolupráce může zahrnovat výměny informací mezi dotčenými příslušnými orgány a žádosti o přijetí kontrolních opatření podle odstavce 2.
			Čl. 4 odst. 3	3) „národní strategií pro bezpečnost sítí a informačních systémů“ rámec vymezující strategické cíle a priority v oblasti bezpečnosti sítí a informačních systémů na vnitrostátní úrovni;
			Článek 14 odst. 7	7. Příslušné orgány jednající společně v rámci skupiny pro spolupráci mohou vypracovat a přijmout pokyny týkající se okolností, za nichž jsou provozovatelé základních služeb povinni hlásit incidenty, včetně parametrů pro určení významnosti dopadu daného incidentu, jak je uvedeno v odstavci 4.
§ 22a	**Určení provozovatele základní služby a informačního systému základní služby** (1) Úřad rozhodnutím určí provozovatele základní služby a informační systém základní služby, pokud naplní odvětvová a dopadová kritéria, která zohledňují významnost a) služeb poskytovaných v jednotlivých odvětvích uvedených v § 2 písm. i) a b) dopad kybernetického bezpečnostního incidentu zejména na 1. rozsah a kvalitu poskytování základní služby uživatelům, kteří jsou na ní závislí, 2. ekonomické a společenské činnosti a	32016L1148	Čl. 5 odst. 1 až 5 a 7	1. Do 9. listopadu 2018 členské státy v každém odvětví a pododvětví uvedeném v příloze II určí provozovatele základních služeb usazené na jejich území. 2. Kritéria pro určení provozovatele základních služeb podle čl. 4 bodu 4 jsou tato: a) subjekt poskytuje službu, která je základní z hlediska zachování kritických společenských nebo ekonomických činností; b) poskytování dotyčné služby je závislé na sítích a informačních systémech a c) incident by vedl k významnému narušení poskytování této služby. 3. Pro účely odstavce 1 sestaví každý členský

	veřejnou bezpečnost, 3. vzájemnou závislost odvětví uvedených v § 2 písm. i). Dopadová a odvětvová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností stanoví prováděcí právní předpis. (2) V případě, že Úřad zjistí, že orgán nebo osoba, které hodlá určit podle odstavce 1 jako provozovatele základní služby, poskytují danou službu i v jiném členském státě, provede před rozhodnutím ve věci konzultaci s příslušným orgánem dotčeného členského státu. (3) Proti rozhodnutí Úřadu o určení provozovatele základní služby a informačního systému základní služby není rozklad přípustný. (4) Úřad ověřuje nejméně každé 2 roky ode dne vydání rozhodnutí o určení provozovatele základní služby, zda jsou splněny podmínky pro určení provozovatele základní služby a informačního systému základní služby.			stát seznam služeb uvedených v odst. 2 písm. a). 4. V případě, že jeden subjekt poskytuje službu uvedenou v odst. 2 písm. a) ve dvou či více členských státech, zahájí tyto členské státy pro účely odstavce 1 vzájemné konzultace. Tyto konzultace proběhnou před přijetím rozhodnutí o určení provozovatele základní služby. 5. Seznam určených provozovatelů základních služeb členské státy pravidelně, a to alespoň každé dva roky ode dne … [21 měsíců ode dne vstupu této směrnice v platnost], přezkoumávají a v případě potřeby jej aktualizují. 7. Pro účely přezkumu uvedeného v článku 23 členské státy do … [27 měsíců ode dne vstupu této směrnice v platnost] a poté každé dva roky předkládají Komisi informace, jež Komise potřebuje k hodnocení provádění této směrnice, zejména z hlediska konzistentnosti přístupů členských států v otázce určování provozovatelů základních služeb. Tyto informace zahrnují alespoň: a) vnitrostátní opatření umožňující určení provozovatelů základních služeb; b) seznam služeb uvedený v odstavci 3; c) počet provozovatelů základních služeb určených v každém odvětví podle přílohy II a jejich význam ve vztahu k dotyčnému odvětví; d) mezní hodnoty, existují-li, pro stanovení příslušné zásobovací úrovně podle počtu uživatelů závislých na dané službě podle čl. 6 odst. 1 písm.

				a) nebo významu konkrétního provozovatele základních služeb podle čl. 6 odst. 1 písm. f). V zájmu větší srovnatelnosti poskytovaných informací může Komise s maximálním ohledem na stanovisko agentury ENISA přijmout patřičné technické pokyny upravující parametry informací uvedených v tomto odstavci.
			Čl. 4 odst. 4	4) „provozovatelem základních služeb“ veřejný nebo soukromý subjekt, jehož druh je uveden v příloze II a jenž splňuje kritéria stanovené v čl. 5 odst. 2;
			Čl. 6	1) Při určování významnosti narušení podle čl. 5 odst. 2 písm. c) členské státy zváží alespoň tyto okolnosti působící napříč odvětvími: a) počet uživatelů, kteří jsou závislí na službě poskytované daným subjektem; b) závislost dalších odvětví podle přílohy II na službě poskytované daným subjektem; c) možný dopad incidentů, pokud jde o jejich intenzitu a délku trvání, na ekonomické a společenské činnosti nebo na veřejnou bezpečnost; d) podíl daného subjektu na trhu; e) zeměpisný rozsah oblasti, která by mohla být incidentem dotčena; f) důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k dostupnosti alternativních způsobů zajištění této služby.

				2) Při posuzování toho, zda by incident vedl k významnému narušení, členské státy případně zváží rovněž okolnosti specifické pro jednotlivá odvětví.
§ 23	Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, jak orgány a osoby uvedené v § 3 písm. a) až g) plní povinnosti stanovené tímto zákonem a rozhodnutími a opatřeními obecné povahy vydanými Úřadem, a dodržují prováděcí právní předpisy v oblasti kybernetické bezpečnosti. Je-li důvodné podezření, že poskytovatel digitální služby neplní povinnosti stanovené tímto zákonem, provede u něj Úřad kontrolu.	32016L1148	Čl. 15 odst. 1 a 2	1. Členské státy zajistí, aby příslušné orgány měly všechny nezbytné pravomoci a prostředky pro posouzení toho, zda provozovatelé základních služeb dodržují své povinnosti podle článku 14, a s tím souvisejících důsledků pro bezpečnost sítí a informačních systémů. 2. Členské státy zajistí, aby příslušné orgány měly pravomoci a prostředky nezbytné k tomu, aby mohly od provozovatelů základních služeb požadovat poskytnutí: a) informací nezbytných pro posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky; b) dokladů o účinném provádění bezpečnostních politik, jako jsou výsledky bezpečnostního auditu provedeného příslušným orgánem nebo kvalifikovaným auditorem, a v případě kvalifikovaného auditora, aby mohlo být požadováno předložení těchto výsledků včetně podpůrných dokladů příslušnému orgánu. Pokud příslušný orgán žádá o poskytnutí těchto informací nebo dokladů, uvede účel své žádosti a upřesní informace, které jsou požadovány.
			Čl. 17 odst. 1 a 2	1. Členské státy zajistí, aby příslušné orgány v případě potřeby přijaly opatření v rámci následné kontroly, mají-li důkazy o tom, že

				poskytovatel digitálních služeb nesplňuje požadavky stanovené v článku 16. Takové důkazy mohou být předloženy příslušným orgánem jiného členského státu, v němž je služba poskytována. 2. Pro účely odstavce 1 musí mít příslušné orgány nezbytné pravomoci a prostředky, aby mohly od poskytovatelů digitálních služeb požadovat: a) poskytnutí informací potřebných k posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky; b) nápravu případného neplnění požadavků stanovených v článku 16.
§ 24 odst. 2	(2) Pokud je informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, informační systém základní služby nebo významný informační systém pro zjištěné nedostatky bezprostředně ohrožen kybernetickým bezpečnostním incidentem, který jej může významně poškodit nebo zničit, může kontrolní orgán zakázat kontrolovanému orgánu nebo osobě používání tohoto systému anebo jeho části do doby, než bude zjištěný nedostatek odstraněn.	32016L1148	Čl. 15 odst. 3	V návaznosti na posouzení poskytnutých informací nebo výsledků bezpečnostních auditů uvedených v odstavci 2 může příslušný orgán vydat provozovatelům základních služeb závazné pokyn k nápravě zjištěných nedostatků.
§ 25 odst. 3 až 13	(3) Správce informačního nebo komunikačního systému kritické informační infrastruktury nebo významného	32016L1148	Čl. 17 odst. 1 a 2	1. Členské státy zajistí, aby příslušné orgány v případě potřeby přijaly opatření v rámci následné kontroly, mají-li důkazy o tom, že poskytovatel digitálních služeb nesplňuje požadavky stanovené

	informačního systému se dopustí přestupku tím, že neinformuje provozovatele systému podle § 4a odst. 1. (4) Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že neinformuje subjekt zajišťující síť elektronických komunikací podle § 4a odst. 2. (5) Provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že a) nesplní povinnost uloženou Úřadem v rozhodnutí podle § 15a odst. 1, b) nepředá data, provozní údaje a informace podle § 6a odst. 2, c) nepředá data, provozní údaje a informace podle § 6a odst. 3, d) nezničí kopie dat, provozních údajů a informací podle § 6a odst. 3, nebo e) neumožní správci dohled nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3. (6) Orgán nebo osoba zajišťující významnou síť se dopustí přestupku tím, že neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 3. (7) Správce a provozovatel informačního systému základní služby se dopustí přestupku tím, že			v článku 16. Takové důkazy mohou být předloženy příslušným orgánem jiného členského státu, v němž je služba poskytována. 2. Pro účely odstavce 1 musí mít příslušné orgány nezbytné pravomoci a prostředky, aby mohly od poskytovatelů digitálních služeb požadovat: a) poskytnutí informací potřebných k posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky; b) nápravu případného neplnění požadavků stanovených v článku 16.

	a) v rozporu s § 4 odst. 2 nezavede nebo neprovádí bezpečnostní opatření nebo nevede bezpečnostní dokumentaci, b) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 4, c) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3, d) nesplní povinnost uloženou Úřadem podle § 13 nebo 14, e) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b), nebo f) nesplní některou z povinností uloženou nápravným opatřením podle § 24. (8) Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury, správce nebo provozovatel významného informačního systému, správce nebo provozovatel informačního systému základní služby a provozovatel základní služby, kteří jsou orgánem veřejné moci, se dopustí přestupku tím, že uzavřou smlouvu s poskytovatelem služeb cloud computingu v rozporu s § 4 odst. 5. (9) Správce nebo provozovatel informačního			

	nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3. (10) Provozovatel základní služby se dopustí přestupku tím, že a) neinformuje správce nebo provozovatele informačního systému základní služby podle § 4a odst. 3, b) nenahlásí významný dopad na kontinuitu poskytování základní služby podle § 8 odst. 1 a 4, c) nenahlásí významný dopad na kontinuitu poskytování základní služby způsobený kybernetickým bezpečnostním incidentem podle § 8 odst. 8, d) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3, nebo e) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b). (11) Poskytovatel digitální služby se dopustí přestupku tím, že a) neustaví svého zástupce podle § 3a odst. 1,			

	b) v rozporu s § 4 odst. 3 nezavede nebo neprovádí bezpečnostní opatření, c) nenahlásí kybernetický bezpečnostní incident podle § 8 odst. 2 a 3, d) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3, nebo e) neoznámí kontaktní údaje podle § 16 odst. 2 písm. a). (12) Za přestupek lze uložit pokutu do a) 5 000 000 Kč, jde-li o přestupek podle odstavce 2 písm. a), odstavce 7 písm. a) nebo odstavce 11 písm. b), b) 1 000 000 Kč, jde-li o přestupek podle odstavce 1, odstavce 2 písm. b), c) nebo e), odstavce 3, odstavce 4, odstavce 5 písm. a), c) nebo d), odstavce 6, odstavce 7 písm. b) až d) nebo f), odstavce 8, odstavce 9, odstavce 10 písm. a) až d) nebo odstavce 11 písm. a), c) nebo d), c) 200 000 Kč, jde-li o přestupek podle odstavce 5 písm. b) nebo e). d) 10 000 Kč, jde-li o přestupek podle odstavce 2 písm. d), odstavce 7 písm. e), odstavce 10 písm. e) nebo odstavce 11			

	písm. e).		Čl. 15 odst. 1 a 2	1. Členské státy zajistí, aby příslušné orgány měly všechny nezbytné pravomoci a prostředky pro posouzení toho, zda provozovatelé základních služeb dodržují své povinnosti podle článku 14, a s tím souvisejících důsledků pro bezpečnost sítí a informačních systémů. 2. Členské státy zajistí, aby příslušné orgány měly pravomoci a prostředky nezbytné k tomu, aby mohly od provozovatelů základních služeb požadovat poskytnutí: a) informací nezbytných pro posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky; b) dokladů o účinném provádění bezpečnostních politik, jako jsou výsledky bezpečnostního auditu provedeného příslušným orgánem nebo kvalifikovaným auditorem, a v případě kvalifikovaného auditora, aby mohlo být požadováno předložení těchto výsledků včetně podpůrných dokladů příslušnému orgánu. Pokud příslušný orgán žádá o poskytnutí těchto informací nebo dokladů, uvede účel své žádosti a upřesní informace, které jsou požadovány.
			Čl. 21	Členské státy stanoví sankce za porušení vnitrostátních právních předpisů přijatých podle této směrnice a přijmou veškerá opatření nezbytná k zajištění jejich uplatňování. Stanovené sankce musí být účinné, přiměřené a odrazující.

				Členské státy oznámí takto stanovené sankce a daná opatření Komisi do dne 9. května 2018 a neprodleně jí oznámí všechny následné změny, jež se těchto ustanovení a opatření týkají.
§ 28 odst. 2 písm. b) a e)	(2) Úřad stanoví vyhláškou b) typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů a náležitosti a způsob hlášení kybernetického bezpečnostního incidentu podle § 8 odst. 7, e) dopadová a odvětvová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1.	32016L1148	Čl. 5 odst. 1 až 3	1. Do 9. listopadu 2018 členské státy v každém odvětví a pododvětví uvedeném v příloze II určí provozovatele základních služeb usazené na jejich území. 2. Kritéria pro určení provozovatele základních služeb podle čl. 4 bodu 4 jsou tato: subjekt poskytuje službu, která je základní z hlediska zachování kritických společenských nebo ekonomických činností; poskytování dotyčné služby je závislé na sítích a informačních systémech; a incident by vedl k významnému narušení poskytování této služby. 3. Pro účely odstavce 1 sestaví každý členský stát seznam služeb uvedených v odst. 2 písm. a).
			Čl. 4 odst. 4	4) „provozovatelem základních služeb“ veřejný nebo soukromý subjekt, jehož druh je uveden v příloze II a jenž splňuje kritéria stanovené v čl. 5 odst. 2;
			Čl. 1 odst. 2 písm. d)	Za tímto účelem tato směrnice: d) zavádí bezpečnostní požadavky a požadavky na hlášení incidentů pro provozovatele základních služeb a pro poskytovatele digitálních služeb;

			Čl. 14 odst. 3 až 4	3. Členské státy zajistí, aby provozovatelé základních služeb hlásili příslušnému orgánu nebo týmu CSIRT bez zbytečného prodlení incidenty se závažným dopadem na kontinuitu základních služeb, které poskytují. Hlášení zahrnuje informace, které příslušnému orgánu nebo týmu CSIRT umožní posoudit případný přeshraniční dopad daného incidentu. Ohlášení nezakládá u oznamující strany vyšší míru právní odpovědnosti. 4. Při posuzování významnosti dopadu incidentu se zohlední zejména tyto parametry: a) počet uživatelů postižených narušením základní služby; b) délka trvání incidentu; c) zeměpisný rozsah oblasti dotčené incidentem.
			Čl. 16 odst. 3 a 4	3. Členské státy zajistí, aby poskytovatelé digitálních služeb bez zbytečného odkladu hlásili příslušnému orgánu nebo týmu CSIRT incidenty, které mají významný dopad na poskytování služby uvedené v příloze III, kterou nabízejí v rámci Unie. Hlášení musí obsahovat takové informace, které příslušnému orgánu nebo týmu CSIRT umožní posoudit významnost případného přeshraničního dopadu daného incidentu. Ohlášení nezakládá u oznamující strany vyšší míru právní odpovědnosti. 4. Při posuzování toho, zda je dopad incidentu významný, se zohlední zejména tyto parametry: a) počet uživatelů postižených incidentem,

				zejména těch uživatelů, kteří na službu spoléhají při poskytování vlastních služeb; b) délka trvání incidentu; c) zeměpisný rozsah oblasti dotčené incidentem; d) rozsah, v jakém bylo narušeno fungování služby; e) rozsah dopadu na společenské a ekonomické činnosti. Ohlášení incidentu je povinné, pouze pokud má poskytovatel digitální služby přístup k informacím, které jsou nezbytné k posouzení dopadu incidentu na základě parametrů uvedených v prvním pododstavci.
			Čl. 1 odst. 6	6. Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti.
			Čl. 3	Aniž je dotčen čl. 16 odst. 10 a aniž jsou dotčeny povinnosti členských států podle práva Unie, mohou členské státy přijímat nebo ponechat v platnosti ustanovení, jejichž cílem je dosáhnout vyšší úrovně bezpečnosti sítí a informačních systémů.

§ 33 odst. 3 a 4	(3) Tento zákon se vztahuje pouze na poskytovatele digitální služby, který je právnickou osobou a není mikropodnikem nebo malým podnikem[15)]. (4) Tento zákon se nevztahuje na poskytovatele digitální služby, který má sídlo v jiném členském státě. _____ [15)] Příloha doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.		Čl. 6 odst. 6 Čl. 16 odst. 11	6) „poskytovatelem digitálních služeb“ jakákoli právnická osoba poskytující digitální službu; 11. Kapitola V se nevztahuje na mikropodniky a malé podniky ve smyslu doporučení Komise 2003/361/ES .
Přechodná ustanovení	**Přechodná ustanovení** 1. Úřad určí provozovatele základní služby a informační systém základní služby podle § 22a odst. 1 zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, do 9. listopadu 2018. 2. Orgány a osoby uvedené v § 3 písm. f) zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, a) oznámí Úřadu do 30 dnů ode dne, kdy byly informovány podle § 4a odst. 3 zákona č. 181/2014 Sb., ve znění ode dne nabytí účinnosti tohoto zákona, kontaktní údaje podle § 16 odst. 1 zákona č. 181/2014 Sb. ve znění účinném ke dni nabytí účinnosti tohoto zákona, a b) začnou nejpozději do 1 roku ode dne, kdy byly informovány podle § 4a odst. 3 zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, plnit ostatní	32016L1148	Čl. 5 odst. 1	1. Do 9. listopadu 2018 členské státy v každém odvětví a pododvětví uvedeném v příloze II určí provozovatele základních služeb usazené na jejich území.

	povinnosti podle zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona. 3. Poskytovatel digitální služby a) oznámí Úřadu nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona kontaktní údaje podle § 16 odst. 1 zákona č. 181/2014 Sb. ve znění účinném ke dni nabytí účinnosti tohoto zákona, a, b) začne nejpozději do 1 roku ode dne nabytí účinnosti tohoto zákona plnit ostatní povinnosti podle zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona. 4. Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny, v případě že podmínky jejich smluvního vztahu uzavřeného s dodavatelem pro jejich informační nebo komunikační systém nesplňují požadavky podle zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, a jeho prováděcích předpisů, uvést smluvní vztah do souladu s těmito požadavky do 1 roku ode dne nabytí účinnosti tohoto zákona.		Čl. 25 odst. 1	Členské státy do 9. května 2018 přijmou a zveřejní právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí. Znění těchto předpisů neprodleně sdělí Komisi. to předpisy ode dne 10. května 2018. pisy přijaté členskými státy musí obsahovat odkaz

				na tuto směrnici nebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsob odkazu si stanoví členské státy.
Účinnost	Tento zákon nabývá účinnosti prvním dnem druhého kalendářního měsíce po jeho vyhlášení.	32016L1148	Čl. 25 odst. 1	1. Členské státy do 9. května 2018 přijmou a zveřejní právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí. Znění těchto předpisů neprodleně sdělí Komisi. Použijí tyto předpisy ode dne 10. května 2018. Tyto předpisy přijaté členskými státy musí obsahovat odkaz na tuto směrnici nebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsob odkazu si stanoví členské státy.

Číslo předpisu EU (kód celex)	Název předpisu EU
32016L1148	Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
32016R0679	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)